



151 Southhall Lane, Ste 450  
Maitland, FL 32751  
P.O. Drawer 200  
Winter Park, FL 32790-0200  
www.inteserra.com

February 12, 2019  
**Via ECFS Filing**

Ms. Marlene H. Dortch, FCC Secretary  
Federal Communications Commission  
9050 Junction Drive  
Annapolis Junction, MD 20701

RE: Native Network, Inc.  
EB Docket No. 06-36; CY2018

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2018 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009 (e) submitted on behalf of the Native Network, Inc.

Any questions you may have regarding this filing should be directed to my attention at 407-740-3006 or via email to [croesel@inteserra.com](mailto:croesel@inteserra.com). Thank you for your assistance in this matter.

Sincerely,

/s/ Carey Roesel

Carey Roesel  
Consultant

cc: Jenny Rickel - Native Network  
tms: FCCx1901

Enclosures  
CR/gs

**EB Docket 06-36**

**Attachments:** Accompanying Statement explaining CPNI procedures

**Attachment A**  
**Statement of CPNI Procedures and Compliance**

## Statement of CPNI Procedures and Compliance

### Use of CPNI

Native Network, Inc. does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Native Network, Inc. has trained its personnel not to use CPNI for marketing purposes. Should Native Network, Inc. elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

### PROTECTION OF CPNI/ALL COMPANIES

Native Network, Inc. has put into place processes to safeguard its customers' CPNI from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI.

### IF COMPANY USES CPNI:

Native Network, Inc. ensures that all access to CPNI be approved by a supervisor with knowledge of the FCC's CPNI requirements. Native Network, Inc. has instituted training procedures and a corresponding disciplinary process to ensure that its personnel understand and comply with restrictions regarding the use and disclosure of, and access to, CPNI.

### DISCLOSURE OF CALL DETAIL OVER PHONE\ALL COMPANIES

Native Network, Inc. does not disclose CPNI over the telephone in response to a customer-initiated telephone inquiry, unless the customer can provide the call detail information that is the subject of the inquiry without the assistance of a customer service representative. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

Native Network, Inc. has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information.

Native Network, Inc. has put into place procedures to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information.

### DISCLOSURE OF CPNI ONLINE\ALL COMPANIES

Native Network, Inc. does not disclose CPNI on-line. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.



**DISCLOSURE OF CPNI AT RETAIL LOCATIONS\ALL COMPANIES**

Native Network, Inc. does not have any retail locations and therefore does not disclose CPNI in-store.

**NOTIFICATION TO LAW ENFORCEMENT/ALL COMPANIES**

Native Network, Inc. has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement.

Native Network, Inc. maintains electronic records of all breaches discovered and notifications made to the USSS and the FBI, and to customers.

**ACTIONS AGAINST DATA BROKERS/ALL COMPANIES**

Native Network, Inc. has not taken any actions against data brokers in the last year.

**CUSTOMER COMPLAINTS ABOUT CPNI BREACHES/ALL COMPANIES**

Native Network, Inc. did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2018.

**INFORMATION ABOUT PRETEXTERS/ALL COMPANIES**

Native Network, Inc. has not developed any information with respect to the processes pretexters are using to attempt to access CPNI but does take steps to protect CPNI by having encrypted databases and firewall and VPN protections.